Attorney Docket No. P14068-US2
Customer Number 27045

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A method for providing controlled access to a desired function in a system ~~which~~ that includes a plurality of functions~~, each of said plurality of functions having a corresponding key associated therewith~~, the method comprising:

dividing the plurality of functions into a plurality of groups;

assigning a corresponding key to each group;

receiving an access request from an external entity, said access request including one of the assigned keys;

~~selecting a key corresponding to said desired function;~~

conducting an authentication process ~~which includes~~ for the external entity, using ~~said selected~~ the key received in the access request; and

~~controlling access to said desired function according to a result of said authentication process~~

upon positively authenticating the external entity, granting the entity access only to the functions in the group corresponding to the key received in the access request, while prohibiting access to functions in other groups.

2. (Canceled)

3. (Original) The method according to claim 1, wherein each of said corresponding keys comprises a public key.

4. (Original) The method according to claim 1, wherein each of said corresponding keys, an authentication code and codes for said plurality of functions are stored in a memory of said system.

5. (Original) The method according to claim 4, wherein said memory comprises an internal read-only memory (IROM).

6. (Original) The method according to claim 4, wherein said memory comprises a one-time programmable part of a non-volatile program memory.

7. (Currently Amended) The method according to claim 1, wherein said step of conducting an authentication process ~~comprises the step of~~ includes conducting a first authentication process ~~which includes~~ using ~~a first selected key~~ the key received in the access request, and wherein said method further ~~includes the step of~~ comprises conducting a second authentication process ~~which includes~~ using a second key, which is generated using a second key code created during the first authentication process.

8. (Currently Amended) The method according to claim 7, wherein said second key comprises a session key computed by said system and [[an]] the external entity seeking access ~~to said desired function~~.

9. (Currently Amended) The method according to claim 8, wherein said second authentication process includes comparing said session keys computed by ~~said~~ the system and ~~said~~ the external entity, wherein access to ~~said desired function~~ the corresponding group of functions by said entity ~~being~~ is authorized only if said compared session keys match.

10. (Original) The method according to claim 8, wherein said second key code is created using a random challenge sent to said entity by said system during the first authentication process.

11. (Original) The method according to claim 7, wherein said second key is stored in a protected static random access memory (PSRAM) of said system.

12. (Currently Amended) ~~The method according to claim 8, wherein said method further includes the step of~~ A method for providing controlled access to a desired function in a system that includes a plurality of functions, each of the plurality of functions having a corresponding key associated therewith, the method comprising:

selecting a key corresponding to the desired function;

conducting a first authentication process using the selected key;

conducting a second authentication process using a second key, which is generated using a second key code created during the first authentication process, said second key being a session key computed by the system and an entity seeking access to the desired function;

controlling access to the desired function according to a result of the authentication process; and

encrypting and decrypting data sent between the entity and the system using the session key.

13. (Original) The method according to claim 12, wherein an algorithm code for the encryption and decryption of data is stored in an internal read-only memory (IROM) of said system.

14. (Original) The method according to claim 12, wherein an algorithm code for the encryption and decryption of data is stored in a one-time programmable part of a non-volatile program memory of said system.

15. (Original) The method according to claim 12, wherein an algorithm code for the encryption and decryption of data is stored in said entity.

16. (Currently Amended) The method according to claim 8, wherein said method further includes the step of adding ~~MAC~~ Message Authentication Code (MAC) protection for data transmitted between the system and the entity, said MAC protection utilizing said session key.

17. (Original) The method according to claim 16, wherein an algorithm code for MAC protection is stored in an internal read-only memory (IROM) of said system.

18. (Original) The method according to claim 16, wherein an algorithm code for MAC protection is stored in a one-time programmable part of a non-volatile program memory of said system.

19. (Original) The method according to claim 16, wherein an algorithm code for MAC protection is stored in said entity.

20. (Original) The method according to claim 1, wherein said system comprises a cellular telephone system.

21-27. (Canceled)

28. (Currently Amended) ~~The method according to claim 22, wherein said method further includes the step of~~ A method for providing controlled access to a desired function in a system that includes one or more functions, said method comprising:

conducting a first authentication process with an external entity using a public key corresponding to the desired function;

conducting a second authentication process using a private session key, which is shared by the system and the external entity, and is generated based on a random challenge made by the system to the external entity during the first authentication process;

controlling access to the desired function according to a result of the first and second authentication processes; and

encrypting and decrypting data sent between the external entity and the system using the private session key.

29. (Original) The method according to claim 28, wherein an algorithm code for the encryption and decryption of data is stored in an internal read-only memory (IROM) of said system.

30. (Original) The method according to claim 28, wherein an algorithm code for the encryption and decryption of data is stored in a one-time programmable part of a non-volatile program memory of said system.

31. (Original) The method according to claim 28, wherein an algorithm code for the encryption and decryption of data is stored in said external entity.

32-36. (Canceled)

37. (Currently Amended) An apparatus for providing controlled access to a desired function in a system ~~which~~ that includes a plurality of functions, said apparatus comprising:

means for dividing the plurality of functions into a plurality of groups;

a memory for storing a plurality of corresponding keys, each key ~~corresponding to one of said plurality of functions; and~~ being assigned to a different group of functions;

means for receiving an access request from an external entity, said access request including one of the assigned keys; and

a processor ~~which conducts~~ for conducting an authentication process for the external entity using ~~a key of said plurality of keys in said memory which corresponds to said desired function, and which controls access to said desired function according to a result of said authentication process~~ the key received in the access request, and upon positively authenticating the external entity, granting the entity access only to the functions in the group corresponding to the key received in the access request, while prohibiting access to functions in other groups.

38. (Currently Amended) The apparatus according to claim 37, wherein said plurality of keys ~~comprise~~ comprises public keys.

39. (Original) The apparatus according to claim 37, wherein said memory comprises an internal read-only memory (IROM).

40. (Original) The apparatus according to claim 37, wherein said memory comprises a one-time programmable part of a non-volatile program memory.

41. (Currently Amended) The apparatus according to claim 37, wherein ~~said authentication process comprises~~ the processor conducts a first authentication process using ~~a first key~~ the key received in the access request, and wherein said processor further conducts a second authentication process using a second key which is generated using a second key code created during the first authentication process.

42. (Currently Amended) The apparatus according to claim 41, wherein said second key comprises a shared session key shared by said system and [[an]] the external entity seeking access ~~to said desired function~~.

43. (Original) The apparatus according to claim 41, wherein said second key is stored in a protected random access memory (PSRAM) of said system.

44. (Original) The apparatus according to claim 37, wherein said system comprises a cellular telephone system.

45-50. (Canceled)

51. (New) The method according to claim 1, wherein the plurality of groups of functions are of different hierarchical levels, wherein access to a higher level provides access to the functions associated with the higher level and to the functions associated with all lower levels.

52. (New) The apparatus according to claim 37, wherein the plurality of groups of functions are of different hierarchical levels, wherein access to a higher level provides access to the functions associated with the higher level and to the functions associated with all lower levels.